

Příloha č. 1 Smlouvy

Klasifikace: Veřejný dokument



Příloha č. 1 zadávací dokumentace veřejné zakázky s názvem „Vzdělávací platforma kybernetické bezpečnosti“

Technická specifikace

Obsah

1	Seznam zkratk	2
2	Úvod	3
2.1	Záměr SŽ v oblasti Vzdělávací platformy kybernetické bezpečnosti Správy železnic, s.o.	3
2.2	Předmět plnění veřejné zakázky	4
3	Technické podmínky zakázky	4
4	Současný stav a popis prostředí	6
5	Požadavky na plnění	6
6	Fáze plnění a akceptační milníky	11
6.1	Fáze 1: Provedení Díla	12
6.1.1	Etapa 1: Příprava implementace	12
6.1.2	Etapa 2: Implementace Díla	14
6.1.3	Etapa 3: Pilotní provoz	14
6.2	Fáze 2: Údržba, provoz a rámcový rozvoj Díla po dobu tří let	16
6.2.1	Údržba a provoz („Paušální služby“)	16
6.2.2	Rámcový rozvoj (dále jen „Služby rozvoje“)	16

1 Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

Zkratka	Popis
AAD	Azure Active Directory
ČSN	Česká státní norma
EN	Evropská norma
EU	Evropská unie
GDPR	General Data Protection Regulation – NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
ICT	Informační a komunikační technologie
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KBI	Kybernetický bezpečnostní incident
KBU	Kybernetická bezpečnostní událost
MD	Man day
SaaS	Software as a service
SLA	Service Level Agreement
SW	Software
SŽ	Správa železnic, státní organizace
VKB	Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
WCAG	Web Content Accessibility Guidelines
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávacího řízení ve vztahu k veřejné zakázce, jejímž předmětem bude dodávka, implementace a provoz softwarového řešení "Vzdělávací platformy kybernetické bezpečnosti Správy železnic, s.o." (dále také jako „Systém“, „Dílo“ nebo „Řešení“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“). Dokument obsahuje popis business požadavků SŽ na Systém a zároveň je posláním dokumentu stanovit a popsat funkční i nefunkční požadavky na Systém.

2.1 Záměr SŽ v oblasti Vzdělávací platformy kybernetické bezpečnosti Správy železnic, s.o.

Hlavním záměrem je doplnění stávajícího řešení vzdělávání kybernetické bezpečnosti zaměstnanců SŽ, tedy klasického statického e-learningového školení v oblasti kybernetické bezpečnosti SŽ.

Zadavatel plánuje implementovat Systém, který dlouhodobě bude zvyšovat povědomí o informační a kybernetické bezpečnosti pomocí krátkých mikrolearningů na jednotlivá témata kybernetické bezpečnosti a phishingového simulátoru, který umožní provádět cílené a sofistikované phishingové kampaně napodobující reálné podvodné kybernetické útoky, které motivují zaměstnance k lepším provozním výkonům, a to ve smyslu snížení vzniku kybernetických bezpečnostních událostí (dále jen „KBU“) a incidentů (dále jen „KBI“) zaměstnancem a zvýšení počtu hlášení KBU a KBI v oblasti informační a kybernetické bezpečnosti.

Hlavním cílem projektu je dodání Systému. Poptávané řešení musí zajistit vhodné funkční a technické prostředí pro vzdělávání v oblasti kybernetické bezpečnosti jak odborných pracovníků, tak i běžných zaměstnanců.

Implementace Systému v prostředí Správy železnic, s.o. zajistí:

- zvyšování povědomí uživatelů o kybernetických hrozbách a vytvoření podmínek pro včasnou identifikaci hrozby kybernetického útoku souvisejících s pracovní činností,
- možnost aktivně a preventivně minimalizovat možný dopad úspěšného kybernetického útoku,
- modernizovat stávající přístup k vzdělávací činnosti na základě pracovního zařazení zaměstnanců a rizikovosti dané pracovní pozice,
- splnění požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB“) a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „VKB“),
- splnění požadavků nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 (dále jen „GDPR“),
- splnění požadavků zákona č. 110/2019 Sb. o zpracování osobních údajů,
- soulad s normou ČSN EN ISO/IEC 27001:2022.

2.2 Předmět plnění veřejné zakázky

Předmětem veřejné zakázky je provést pro Zadavatele Dílo a poskytnout Zadavateli služby podpory a rozvoje na dobu 3 let. Předmět veřejné zakázky je rozdělen do níže uvedených fází:

- **Fáze 1: Provedení Díla** v následujících na sebe navazujících etapách:
 - Etapa 1: Příprava implementace
 - Etapa 2: Implementace Díla
 - Etapa 3: Pilotní provoz
- **Fáze 2: Údržba, provoz a rámcový rozvoj Systému po dobu 3 let** (dále jen „Služby podpory“) sestávající z následujících činností:
 - Údržba a provoz (dále jen „Paušální služby“)
 - Rámcový rozvoj (dále jen „Služby rozvoje“)

Systém bude obsahovat následující poptávané oblasti definované požadavky:

1. Obecné požadavky
2. Specifické požadavky
3. Technické požadavky
4. Integrovaní požadavky

3 Technické podmínky zakázky

Jednotlivé poptávané oblasti zakázky jsou blíže definovány a popsány v tabulkách níže.

Fragmentarizace požadavků předmětu plnění veřejné zakázky:

Obecné požadavky		
ID	Název požadavku	Popis požadavku
OP1	Cloudové řešení	Řešení postavené na modelu Software as a Service (SaaS).
OP2	Automatické aktualizace	Řešení musí umožňovat automatické nasazení aktualizací.
OP3	Plošné školení koncových uživatelů	Řešení musí umožnit plošné a automatizované proškolení všech koncových uživatelů formou mikrolearningů distribuovaných pomocí e-mailových zpráv adresovaných koncovým uživatelům zadavatele.
OP4	Pokrytí všech běžných situací uživatele	Moduly školení musí zahrnovat témata fyzické i digitální informační bezpečnosti.
OP5	Obsah školení v souladu s nejlepší praxí	Obsah školení musí být prokazatelně v souladu dobrou (nejlepší) praxí.
OP6	Customizace řešení	Řešení musí umožňovat individuální zákaznické customizace.
OP7	Technická podpora řešení	Zhotovitel garantuje vzdálenou podporu minimálně formou e-mailu v režimu 5x8, a to v českém jazyce.
OP8	Jazyková mutace řešení	Řešení musí umožnit uživateli se školit v různých jazycích, a to minimálně v českém a v anglickém jazyce.

OP9	Vytvoření komunikační kampaně	Zhotovitel musí vytvořit interní komunikační kampaň pro Zadavatele.

Specifické požadavky

ID	Název požadavku	Popis požadavku
SP1	Technické hrozby pro netechnické uživatele	Obsah modulů školení musí pokrývat i hrozby, u kterých uživatel z principu nemůže rozumět technické podstatě hrozby.
SP2	Přizpůsobení obsahu	Řešení musí umožňovat přizpůsobení obsahu modulů školení prostřednictvím vlastních textů zadavatele.
SP3	Příklady z praxe	Obsah modulů školení musí prezentovat (obsahovat) i příklady ze skutečné praxe např. phishing, smishing, vishing atp.
SP4	Podpůrné materiály	Obsah modulů školení musí umožňovat přikládat podpůrné školící materiály, které jsou součástí obsahu školení nebo na ně odkazovat. Obsah školení musí být možné vytisknout.
SP5	Časová délka školícího modulu	Doporučená časová doba obsahu školícího modulu (mikrolearningu) se musí pohybovat v rozmezí mezi 5-15 minutami.
SP6	Časová flexibilita	Řešení musí umožňovat uživateli se opakovaně připojit do školícího modulu.
SP7	Administrace řešení	Řešení musí obsahovat administrátorské rozhraní pro správu uživatelů, obsahu školících modulů, simulace podvodných e-mailů a jejich distribuci atp.
SP8	Tvorba skupin uživatelů a přiřazování oprávnění	Řešení musí administrátorovi umožňovat bez dodatečných nástrojů vytvářet a spravovat skupiny a přiřazovat práva pro jednotlivé uživatele či skupiny.
SP9	Školení administrátorů	Zhotovitel proškolí administrátory Zadavatele.
SP10	Reporting	Řešení musí umožňovat administrátorovi zobrazit aktuální stav (vyhodnocení) školení a simulace podvodných e-mailů.
SP11	Rozdělení do modulů	Řešení musí umožnit rozdělení do školících modulů.
SP12	Automatizace	Řešení musí podporovat automatizaci procesů.
SP13	Rozvoj	Řešení musí umožňovat rozvoj na základě specifických požadavků Zadavatele.
SP14	Simulace podvodných e-mailů	Řešení musí umožňovat nástroj pro vytváření a zasílání podvodných e-mailových zpráv.
SP15	Podvodné webové domény	Řešení musí umožňovat vytváření podvodných webových stránek a URL adres (internetových domén).

Technické požadavky

ID	Název požadavku	Popis požadavku
TP1	Tenký klient	Školení musí být dostupné na běžných kancelářských PC, bez nutnosti instalovat jakýkoli software.
TP2	Kompatibilita	Řešení musí být kompatibilní s webovými prohlížeči.
TP3	Uživatelský přístup	Řešení musí umožnit přihlašování pomocí SSO (tzn. Singl Sign On).

TP4	Responzivní design	Řešení musí být plně responzivní.
TP5	Provozní dokumentace	Dodavatel poskytne provozní dokumentaci k dodávanému řešení např. uživatelský manuál, administrátorský manuál atd.
TP6	Přístupnost řešení	Řešení musí být v souladu s Web Content Accessibility Guidelines (WCAG).
TP7	Zálohování	Řešení musí umožňovat kompletní zálohu celého řešení, a to jeho nastavení a obsahu.
TP8	Licence	Součástí ceny řešení jsou uživatelské licence pro použití řešení na dobu tří let.
TP9	Testovací prostředí	Řešení musí zahrnovat testovací prostředí.
TP10	Multifaktorová autentizace pro administrátory	Řešení musí zahrnovat postup pro ověření totožnosti administrátora Zadavatele.

Integrační požadavky

ID	Název požadavku	Popis požadavku
IP1	Automatizovaný import uživatelů	Řešení musí umožňovat automatizovaný import, integraci s AAD.
IP2	Bezpečnostní monitoring	Řešení musí umožňovat napojení a přístup k auditním údajům bezpečnostním nástrojem Zadavatele.

Poznámka – Bližší specifikata jednotlivých požadavků je dále rozpracována v kapitole 6 Požadavky na plnění.

4 Současný stav a popis prostředí

Platforma Správy železnic, státní organizace představuje ucelený dokument Správy železnic, státní organizace, který specifikuje souhrn podporovaných infrastrukturních služeb, komponent, principů a architektonických vzorů. Tímto Platforma SŽ definuje základní rámec aplikovatelný při dodávce a návrhu ICT řešení.

Dokument Platforma SŽ je součástí Zadávacího řízení případně Zadavatel může dokument poskytnut Zhotoviteli, a to na základě písemné žádosti.

Zvláštní obchodní podmínky pro Zakázky v oblasti ICT představuje dokument, který definuje parametry a upřesňuje konkrétní podmínky a specifikace Zadavatele v oblasti ICT zakázek, uvedené je součástí Zadávacího řízení.

5 Požadavky na plnění

V rámci návrhu nového Systému pro vzdělávání zaměstnanců SŽ v oblasti informační a kybernetické bezpečnosti byly identifikovány obecné (hlavní), specifické, technické a integrační požadavky, které jsou detailněji popsány níže.

Obecné požadavky

- **Cloudové řešení** obecný požadavek – OP1

Řešení bude postavené na modelu Software as a Service (dále jen „SaaS“), které bude dostupné z různých uživatelských zařízení zaměstnanců SŽ. Řešení musí být centralizované a jednotné pro všechny organizační složky Zadavatele.

- **Automatické aktualizace** obecný požadavek – OP2

Řešení musí umožňovat plánování automatického nasazení aktualizací dat (obsah). Aktualizace, které odstraňují bezpečnostní problémy nebo nestabilní chování řešení, rozšiřuje či zvyšuje výkon řešení jsou standardně nasazeny bez plánování. Řešení musí být schopno při aktualizaci (update či upgrade) na vyšší verzi automaticky přenést stávající data včetně jejich historie, taktéž historické výstupy a reportingy.

- **Plošné školení koncových uživatel** obecný požadavek – OP3

Řešení musí umožnit plošné a automatizované proškolení koncových uživatelů, a to pomocí mikrolearningových kurzů, které jsou distribuovány pomocí e-mailových zpráv adresovaných koncovým uživatelům zadavatele.

- **Pokrytí všech běžných situací uživatele** obecný požadavek – OP4

Řešení musí obsahovat moduly fyzické i digitální informační a kybernetické bezpečnosti. Moduly školení musí pokrývat témata každodenní pracovní činnosti zaměstnance jako je práce s firemním počítačem, firemním mobilním zařízením, a to i mimo pracoviště, během pracovní cesty i při práci na home office.

- **Obsah školení v souladu s nejlepší praxí** obecný požadavek – OP5

Obsah modulů školení musí být prokazatelně v souladu dobrou praxí reprezentovanou normou ČSN EN ISO/IEC 27001:2022 (příloha A) a 27002:2022, resp. jejím obvyklým promítnutím do požadavků na chování uživatelů.

- **Customizace řešení** obecný požadavek – OP6

Řešení musí umožňovat individuální zákaznické customizace např. možnost upravit dílčí parametry vzhledu, uživatelské ovládání nebo přidání rozšiřitelného školicích modulů či šablon podvodných e-mailů atp.

- **Technická podpora** obecný požadavek – OP7

Zhotovitel garantuje vzdálenou podporu minimálně v režimu 5x8, a to v českém jazyce. Zhotovitel je povinen při provádění Díla a poskytování Služeb podpory respektovat veškeré interní dokumenty SŽ.

- **Jazykové mutace** obecný požadavek – OP8

Řešení musí umožnit uživateli se školit v různých jazycích, a to v minimálně v českém, a v anglickém jazyce. Řešení musí uživateli jednoduše umožnit výběr z uvedených jazyků.

- **Vytvoření interní komunikační kampaně** obecný požadavek – OP9

Zhotovitel musí vytvořit interní komunikační kampaň pro Zadavatele, ve které představí dané řešení a jeho výhody pro uživatele. Interní kampaň musí obsahovat elektronickou i tištěnou verzi interní kampaně pro Zhotovitele.

Specifické požadavky

- **Technické hrozby pro netechnické uživatele** specifické požadavky – SP1

Obsah modulů školení musí pokrývat (popisovat) i hrozby, u kterých uživatel z principu nemůže rozumět technické podstatě hrozby, ale musí být schopen správně reagovat např. útoky na operační systém nebo útoky na kancelářské aplikace.

- **Přízpůsobení obsahu** specifický požadavek – SP2

Řešení musí umožňovat tvorbu, vkládání a editaci textů včetně možnosti vkládání hypertextových odkazů, video, audio, obrázky atp. Texty bude možné vytvářet a editovat přímo v daném řešení, které musí dále umožňovat vkládání jak textových a číselných hodnot, tak i fotografií, obrázků, videí, či zvukových efektů.

- **Příklady z praxe** specifický požadavek – SP3

Řešení a jeho školící moduly (obsah) musí prezentovat i příklady ze skutečné praxe např. phishing, smishing, vishing atp.

- **Podpůrné materiály** specifický požadavek – SP4

Řešení musí umožňovat vkládat či odkazovat na podpůrné materiály a umožnit uživateli buď jejich stažení nebo tisk.

- **Časová délka školícího modulu** specifický požadavek – SP5

Doporučená časová doba obsahu školícího modulu se musí pohybovat v rozmezí mezi 5–15 minutami.

- **Časová flexibilita** specifický požadavek – SP6

Řešení musí umožňovat uživateli kdykoli se připojit do školícího modulu.

- **Administrace řešení** specifický požadavek – SP7

Řešení musí obsahovat administrátorské rozhraní pro správu samotného řešení, tedy umožňovat bez dodatečných nástrojů vytvářet, editovat a zpřístupňovat školící moduly a simulaci podvodných e-mailů pro různé skupiny uživatelů.

- **Tvorba skupin uživatelů a přiřazování oprávnění** specifický požadavek – SP8

Řešení musí administrátorovi umožňovat bez dodatečných nástrojů přidávat jednotlivě nebo skupinově uživatele nebo je stejným způsobem odebírat, vytvářet skupiny uživatelů a přiřazovat oprávnění pro jednotlivé uživatele.

- **Školení administrátorů** specifický požadavek – SP9

Zhotovitel proškolí celkem dva administrátory Zadavatele v rámci používání řešení, a to konkrétně v obsluze, tvorbě a administraci řešení a případně dalším, které souvisí s poptávaným řešením.

- **Reporting** specifický požadavek – SP10

Řešení musí umožňovat administrátorovi zobrazit aktuální stav (vyhodnocení) školení a simulace podvodných e-mailů, a to ve smyslu např. úspěš – neúspěš, nahlásil – nenahlásil, míra otevření, míra proklikovosti atp. u všech uživatelů napříč organizací, a to dle skupin, modulů či simulace podvodných e-mailů anebo v detailu jednotlivých uživatelů.

- **Rozdělení do modulů** specifický požadavek – SP11

Řešení musí umožnit členění (rozdělení) školení do různých školicích modulů či úrovní.

- **Automatizace** specifický požadavek – SP12

Řešení musí umožňovat automatizaci procesů, a to např. notifikace uživatelům, plánování spuštění jednotlivých školicích modulů, plánování spuštění simulovaných podvodných e-mailových zpráv.

- **Rozvoj** specifický požadavek – SP13

Řešení musí umožňovat rozvoj na základě specifických požadavků Zadavatele, a to po dobu platnosti smlouvy v rozsahu 20 MD/Rok.

- **Simulace podvodných e-mailů** specifický požadavek – SP14

Řešení musí obsahovat nástroj pro vytváření, plánování, správu a zasílání podvodných e-mailových zpráv. Nástroj musí umožňovat zasílání podvodných e-mailových zpráv, a to minimálně na 6 500 e-mailových kontaktů s možností variabilní změny (snížení, zvýšení), měsíčně umožní rozeslat minimálně 25 000 odeslaných podvodných e-mailů.

Pozn. Vzhledem k fluktuaci zaměstnanců zadavatele nelze zadavatelem přesně určit pevný počet uživatelských licencí.

- **Podvodné webové domény** specifický požadavek – SP15

Řešení musí umožňovat vytvářet podvodné webové stránky a URL adresy (internetových domén).

Technické požadavky

- **Tenký klient** technický požadavek – TP1

Školení musí být dostupné na běžných kancelářských PC, bez nutnosti instalovat jakýkoli software.

- **Kompatibilita** technický požadavek – TP2

Řešení musí být kompatibilní s webovými prohlížeči (nejnovější verze) např. Microsoft Edge, Google Chrome, Safari, Samsung Internet atd.

- **Uživatelský přístup** technický požadavek – TP3

Řešení musí umožnit přihlašování každému zaměstnanci SŽ pomocí jednotného přihlášení SSO (tzn. Singl Sign On) a současně nabídnout alternativní přihlášení pomocí e-mailové adresy.

- **Responzivní design** technický požadavek – TP4

Řešení musí být plně responzivní, tedy flexibilně se přizpůsobí zařízení, na kterém je právě prohlížen, a to na různých typech zobrazovacích zařízení např. mobilní telefon, notebook, tablet atp.

- **Provozní dokumentace** technický požadavek – TP5

Řešení musí obsahovat provozní dokumentaci k dodávanému řešení např. uživatelský manuál, administrátorský manuál, školicí materiály atd.

- **Přístupnost řešení** technický požadavek – TP6

Řešení musí být v souladu s metodikou Web Content Accessibility Guidelines (WCAG), ze které vychází zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací.

- **Zálohování** technický požadavek – TP7

Řešení musí umožňovat kompletní zálohu celého řešení, a to jeho konfigurační nastavení a obsah jednotlivých modulů školení a simulací podvodných e-mailových zpráv atd. Zhotovitel musí vytvořit plány zajištění kontinuity provozu, bezpečnosti, monitoringu, zálohování a odolnosti proti havárii, uvedené bude součástí provozní dokumentace.

- **Licence** technický požadavek – TP8

Součástí ceny řešení jsou uživatelské licence pro použití řešení na dobu tří let, a to včetně poplatku za technickou podporu řešení v odhadovaném počtu 6 500 uživatelů s možností variabilní změny (snížení, zvýšení).

Pozn. Vzhledem k fluktuaci zaměstnanců zadavatele nelze zadavatelem přesně určit pevný počet uživatelských licencí.

- **Testovací prostředí** technický požadavek – TP9

Řešení musí zahrnovat testovací prostředí zřízeném Zhotovitelem. Testovací prostředí bude využito při implementaci, testování a nasazování změn atp.

Integrační požadavky

- **Automatizovaný import** integrační požadavek – IP1

Řešení musí umožňovat automatizovaný import, integraci s AAD. Řešení musí podporovat jednotné přihlášení SSO.

- **Bezpečnostní monitoring** integrační požadavek – IP2

Řešení musí umožňovat Zadavateli integraci (napojení) a přístup k auditním údajům bezpečnostním nástrojem Zadavatele.

OMEZENÍ DEFINOVANÝCH POŽADAVKŮ

Definovanými požadavky Zadavatelem nezaručují 100% taxativní výčet veškerých možných a uvažovaných požadavků na poptávané řešení, neboť nelze ze strany Zadavatele identifikovat veškeré myslitelné požadavky.

Vzhledem k výše uvedenému lze očekávat, že Zadavatel může v průběhu provádění Díla vznést či doplnit požadavky.

Pro vyloučení pochybností Zadavatel uvádí, že následující oblast **NENÍ** předmětem plnění (dodávky) veřejné zakázky:

- Hardware pro provoz řešení (Systému) a
- Licence Microsoft

Pro provoz řešení Zhotovitel poskytne hardwarové a softwarové zdroje.

6 Fáze plnění a akceptační milníky

Předmětem veřejné zakázky je provést pro Zadavatele Dílo a poskytnout Zadavateli Služby podpory a rozvoje na dobu tří let. Předmět veřejné zakázky je rozdělen do níže uvedených fází:

- **Fáze 1: Provedení Díla** v následujících na sebe navazujících etapách:
 - Etapa 1: Příprava implementace
 - Etapa 2: Implementace Díla
 - Etapa 3: Pilotní provoz
- **Fáze 2: Údržba, provoz a rámcový rozvoj Díla po dobu tří let** (dále jen „Služby podpory“) sestávají z následujících činností:
 - Údržba a provoz (dále jen „Paušální služby“)
 - Rámcový rozvoj (dále jen „Služby rozvoje“)

6.1 Fáze 1: Provedení Díla

6.1.1 Etapa 1: Příprava implementace

Etapa 1: Příprava implementace je rozdělena do dvou na sebe navazujících podetap:

1. Podetapa 1.1: Předimplementační analýza řešení
2. Podetapa 1.2: Dokumentace řešení

a) Podetapa 1.1: Předimplementační analýza řešení

Zpracování předimplementační analýzy pro navrhované (poptávané) řešení, a to v tom směru, že Zhotovitel ověření zejména možnosti napojení na související ICT prostředí a systémy Správy železnic, státní organizace pro potřeby jednoznačné identifikaci, import a vytvoření uživatelských účtů (zaměstnanců) a nastavení příslušných procesů v navrhovaném (poptávaném) řešení.

Předimplementační analýza bude také obsahovat detailní návrh řešení a prováděcí harmonogram včetně jednotlivých kroků, definici požadavků na součinnost ze strany Zadavatele a návrh metodiky akceptačních funkčních a výkonových (zátěžových) testů a testovacích scénářů testů obnovy řešení.

b) Podetapa 1.2: Dokumentace řešení (cílový koncept)

Zhotovitel zdokumentuje navrhované (poptávané) řešení. Do dokumentu promítne výsledky předimplementační analýzy řešení, kterou Dodavatel v této podetapě zpracuje za účelem rozpoznat a zpracovat všechny aspekty nezbytné pro realizaci.

Analýzu a návrh (poptávaného) řešení zhotovitel provede a v dokumentaci k řešení popíše, a to v souladu s požadavky Zadavatele. Dokumentace řešení musí rozpracovat požadavky Zadavatele a obsahovat detailní popis technického a programového řešení v souladu s touto Zadávací dokumentací.

Cílový koncept bude vhodně strukturován a uspořádán do sady navazujících kapitol či dokumentů, aby potřebné aspekty zachytila srozumitelným a přehledným způsobem ve všech potřebných vazbách a souvislostech a usnadnila tak její akceptaci Zadavatelem ve vší celistvosti.

Minimální požadavky Zadavatele na obsah Cílového konceptu

1. Popis řešení

- Popis současného stavu prostředí Zadavatele a připravenost prostředí i organizace Zadavatele na implementaci nového řešení z pohledu všech souvisejících aspektů.
- Popis fungování řešení (technický návrh řešení, který musí plně zohledňovat příslušnou stávající platnou legislativu České republiky, včetně souvisejících norem ČSN a dodržení standardů SŽ).

- Způsob zajištění funkčních a nefunkčních požadavků na řešení.
 - Architektura řešení, včetně modulů, funkčních celků, popisu a vazeb na okolní systémy.
 - Popis jednotlivých součástí řešení, jejich funkčnost a vzájemné propojení.
 - Návrh rolí a oprávnění v řešení.
 - Návrh datových základů pro řešení (včetně analýzy disponibilních dat Zadavatele a popisu způsobu zajištění/doplnění dat nezbytných pro funkci řešení), návrh datových struktur, datový model.
 - Detailní popis použitého SW a požadavků na výpočetní prostředí, zpracovávané objemy dat, výkonnostní parametry řešení pro jednotlivá výpočetní prostředí.
 - Popis výkonnostních a kapacitních omezení, na něž je řešení dimenzováno, a popis způsobu, jakým bude možno výkonost řešení dále rozšiřovat formou rozšiřování technického vybavení, konfigurování či doplňování software, zaměňování či doplňování licencí apod.
 - Popis integrací řešení na další aplikační řešení Zadavatele, popis komunikace s externími systémy.
 - Specifikace průběhu migrace dat ze stávajících systémů Zadavatele, popis všech datových zdrojů pro migraci, dílčí fáze migrace a postupy vedoucí k ověření správnosti této migrace (migrační scénář).
 - Popis konfigurace řešení pro prostředí Zadavatele.
 - Popis výkonnostních a kapacitních parametrů řešení.
 - Přehled možností budoucího rozšiřování řešení.
 - Popis zajištění kontinuity, bezpečnosti, monitoringu a zálohování v návaznosti na popis architektury.
 - Popis zabezpečení komunikace, bezpečnostní požadavky a opatření, popis dostupnosti.
2. Implementace řešení
- Popis nasazení řešení včetně definice pilotního provozu.
 - Strategie testování, definice testovacích scénářů, popis průběhu testování a akceptace, včetně výstupů.
 - Detailní popis akceptačních kritérií.
 - Strategie školení – přehled školení, doba trvání, osnovy, popis.
 - Další informace potřebné pro zajištění implementace, testování a provozu.
3. Dokumentace řešení
- Uživatelská dokumentace.
 - Systémová a administrátorská dokumentace.
 - Školící materiály.
 - Provozní dokumentace.
4. Způsob a rozsah poskytování Paušálních služeb
- Koncept budoucího provozního modelu, provozování, správy, administrace, dohledu a servisování řešení včetně záručního a pozáručního servisu.
 - Popis zajištění kontinuity provozu, bezpečnosti, monitoringu, zálohování a odolnosti proti havárii ve vazbě na popis architektury.
 - SLA a způsob jejich monitoringu zajišťovaného Dodavatelem.

- Disaster recovery řešení.
 - Fungování a způsob komunikace s HelpDesk Zhotovitele.
5. Způsob poskytování Služeb rozvoje
 6. Způsob poskytování Součinnosti při ukončení, reimplementaci či migraci dat do jiného prostředí

Výstupem podetapy 1.2: Dokumentace řešení (cílový koncept) bude podrobná dokumentace implementace a hrubý časový harmonogram. Výstup podetapy 1.2 podléhá akceptaci ze strany Zadavatele.

6.1.2 Etapa 2: Implementace Díla

Zhotovitel v této etapě postupně v navazujících aktivitách provede implementační práce, které povedou ke splnění požadavků na řešení, a tím bude umožněn následný pilotní provoz řešení v etapě 3.

Etapa 2 je rozdělena tří na sebe navazujících podetap:

- Podetapa 2.1: Propojení řešení s Platformou SŽ
- Podetapa 2.2: Implementace řešení
- Podetapa 2.3: Testování způsobilosti pro Pilotní provoz

a) Podetapa 2.1 Propojení řešení s Platformou Správy železnic, státní organizace

Zhotovitel připraví propojení řešení s integrační Platformou Správy železnic, státní organizace, prostřednictvím které zajistí import uživatelů Správy železnic, státní organizace.

b) Podetapa 2.2 Implementace řešení

V rámci této podetapy proběhne ze strany Zhotovitele zpřístupnění řešení, implementace funkcí dle funkčních požadavků definovaných v kapitole 4 této Technické specifikace a nastavení řešení.

c) Testování způsobilosti pro Pilotní provoz

V rámci této aktivity proběhne testování řešení a jeho způsobilosti pro pilotní provoz řešení v etapě 3 dle předem definovaných testovacích scénářů definovaných v Cílovém konceptu.

6.1.3 Etapa 3: Pilotní provoz

V Etapě 3 bude probíhat pilotní provoz a optimalizace řešení. Pilotní provoz znamená provoz řešení v rozsahu všech jeho funkcionalit. Cílem této etapy je na základě průběžného vyhodnocování pilotního provozu optimalizovat řešení pro možnost akceptace Díla jako celku Zadavatelem.

- Průběh pilotního provozu – v rámci této aktivity bude probíhat Pilotní provoz dle postupu odsouhlaseného v Cílovém konceptu. Zhotovitel bude monitorovat průběh pilotního provozu řešení a průběžně provádět sběr

připomínek Zadavatele k průběhu pilotního provozu. Cílem je ověřit soulad řešení s touto technickou specifikací a se schváleným Cílovým konceptem.

- Vyhodnocení pilotního provozu – Zhotovitel na základě vlastního monitoringu průběhu Pilotního provozu řešení a na základě sběru připomínek identifikovaných Zadavatelem provede vyhodnocení pilotního provozu a návrh optimalizace řešení a zpracuje dokument Vyhodnocení pilotního provozu. Dokument Vyhodnocení pilotního provozu podléhá akceptaci Zadavatele.

Dodavatel v rámci této podetapy zdokumentuje navrhované řešení a jeho jednotlivých technických a softwarových komponent ve formě dokumentace, která umožní správu, provozování, užívání, servis i další rozvoj řešení ve všech jeho vrstvách. Zhotovitel zdokumentuje rovněž integrační služby a datová rozhraní. Zpracuje postupy pro běžný provoz i servisní zásahy a údržbu. Provozní části dokumentace musí svojí mírou úplnosti a podrobnosti umožnit provoz a správu řešení bez přímého bezprostředního zapojení Zhotovitele.

Zhotovitel bude udržovat po dobu trvání Fáze 1 a Fáze 2 dokumentaci v aktuálním stavu, aby zohledňovala úpravy a změny prováděné v průběhu Fáze 1 a Fáze 2. Zhotovitel za tím účelem popíše a nastaví vhodný mechanismus ukládání a aktualizace dokumentace.

Zhotovitel v rámci této podetapy provede školení, která musí pokrývat všechny aspekty práce s řešením, jeho uživatelské a technické služby, provozování procesů a souvisejících činností vykonávaných pracovníky Zadavatele, případně pracovníky dotčených organizací ještě před nasazením do ostrého provozu.

Zhotovitel dále poskytne plnou součinnost a umožní na vyžádání Zadavatele provést bezpečnostní penetrační testování navrhovaného (poptávaného) řešení a případné zranitelnosti či neshody Zhotovitel odstraní.

Po provedení pilotního provozu a bezpečnostních penetračních testů a odstranění případných neshod Zhotovitel převede řešení do ostrého provozu (produkce), a to pro skupinu uživatelů definovanou Zadavatelem a zhotovitel zajistí technickou podporou řešení.

V rámci této fáze Zhotovitel vybuduje také testovací prostředí řešení.

Součástí pilotního provozu a následného převedení do ostrého provozu (produkce) je napojení (integrace) řešení na dohledové bezpečnostní systémy Zadavatele, tedy integraci řešení do Security Incident and Event Management s cílem monitorovat a zaznamenávat aktivity uživatelů a Zhotovitele řešení.

6.2 Fáze 2: Údržba, provoz a rámcový rozvoj Díla po dobu tří let

6.2.1 Údržba a provoz („Paušální služby“)

Zhotovitel bude Zadavateli poskytovat Paušální služby, které představují aktivity Zhotovitele spojené s periodickou a preventivní údržbou řešení, jeho provozem a opravami a dále aktivity poskytování služeb Zhotovitelova centra podpory spolu s poskytováním konzultací.

Zhotovitel je povinen poskytovat Paušální služby kontinuálně po celou dobu platnosti a účinnosti smlouvy, a to ode dne akceptace Fáze 1, tzn. převzetí Díla jako celku Zadavatelem. Typy Paušálních služeb jsou stanoveny ve smlouvě a poskytovány dle jejich vymezení nebo na vyžádání způsobem podle přesně stanovených komunikačních mechanismů.

Zhotovitel vyžaduje v rámci paušálních služeb zajištění pravidelné aktualizace řešení.

6.2.2 Rámcový rozvoj (déle jen „Služby rozvoje“)

Služby rozvoje zahrnují např. následující činnosti:

- Provádění úprav řešení z důvodu změn interních předpisů vztahujících se k řešení v důsledku změn směrnic a jiných interních předpisů Zadavatele, a to vždy na základě požadavku a výhradně na pokyn Zadavatele.
- Vývoj doplňků verzí a nových verzí v souladu s právními předpisy a s tím spojené souběžné rozšiřování funkcionality před nabytím účinnosti nových právních předpisů.
- Implementace nově zpracovaných změnových požadavků do prostředí řešení a zpracování aktualizace související dokumentace spočívající zejména ve zdokumentování provedených změn a úprav do všech úrovní dokumentace řešení a její pravidelná a včasná aktualizace a vytvoření aktuálních návodů a postupů práce v řešení.
- Seznámení vybraných (klíčových) uživatelů a technického personálu s provedenými změnami.
- Zajišťování úprav automatizovaného exportu dat řešení. Tvorba nových výstupů z dat řešení na základě požadavku Zadavatele, doplnění, vylepšení a běžné úpravy stávajících výstupů vyplývající z užívání řešení a dle požadavků Zadavatele.
- Odborné poradenství a technická pomoc při dalším rozvoji řešení.
- Optimalizace postupů v případě, že to provedené úpravy vyžadují, promítnutí realizovaných změn do vytvořených výstupů a datových sestav.

Na doplnění funkcionality a nové verze podle tohoto odstavce se vztahuje záruční doba od podepsání akceptačního protokolu k dané úpravě řešení definovaných dle domluvených záruk.